AO 106 (Rev. 01/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address.)

Google account "daviddblasczak" and associated email address "daviddblasczak@gmail.com"

Case No. 18-MJ- 523

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Western District of New York *(identify the person or describe property to be searched and give its location):* **Google account "daviddblasczak" and associated email address "daviddblasczak@gmail.com"as maintained by Google, Inc., a company with offices located in Mountain View, California, as described in Attachment A.**

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*: **See Attachment B for the Items to be Seized, all of which are evidence and instrumentalities of violations of Title 18 United States Code, Sections 2251(a), 2252A(a)(2)(A) and 2252A(a)(5)(B), and all of which are more fully described in the application and affidavit filed in support of this warrant, the allegations of which are adopted and incorporated by reference as if fully set forth herein.**

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- X evidence of a crime;
- X contraband, fruits of crime, or other items illegally possessed;
- X property designed for use, intended for use, or used in committing a crime;
- ____ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 U.S.C. §§ **2251(a), 252A(a)(2)(A) and 2252A(a)(5)(B)**, and the application is based on these facts which are continued on the attached sheet.

☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Justin Burnham, Special Agent, H.S.I.
Printed name and title

Sworn to before me and signed in my presence.

Date: 1/26/18

Judge's signature

City and state: Rochester, New York

Jonathan W. Feldman, United States Magistrate Judge
Printed name and title

ATTACHMENT A

SUBJECT ACCOUNT

The Google account and associated email address to be searched is a certain account controlled by the internet service provider known as Google, headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043 in the Northern District of California. The account name to be searched belongs to the following Google user:

Email: daviddblasczak@gmail.com

Username: daviddblasczak

ATTACHMENT B

ITEMS TO BE SEIZED

I. Information to be disclosed by Google, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, Google is required to disclose the following information to the government for the account or identifier listed in Attachment A. Such information should include the below-described content of the SUBJECT ACCOUNT, as it was preserved. Your Affiant requests that all electronic information is provided in its original electronic form on a compact disc (CD) or Digital Versatile Disc (DVD).

a. The contents of all electronic mails stored in the account, including copies of electronic mails sent to and from the account, draft electronic mails, attachments, the source and destination addresses associated with each electronic mail, the date and time at which each electronic mail was sent, and the size and length of each electronic mail.

b. Any deleted emails, including information described in subparagraph "a," above.

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative electronic mail addresses provided during registration, other Google accounts that share the same SMS or secondary email address as the target account as well as any other accounts that use the target email address as a secondary email address, methods of connecting, log files, and means and source of payment (including any credit or bank account number).

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files

e. All records pertaining to communications between Google and any person regarding the account, including contacts with support services and records of actions taken.

f. Any documents, folders, folder names and directory listing, images, data, videos and attachments stored within this account or accessible by user daviddblasczak (daviddblasczak@gmail.com). This would also include images, data, videos, documents, posts, and attachments stored in Google Picasa, Google+ including a copy of the Google+ profile and the Google+ Circles and Contacts, Google+ Photos, Google Earth, Google Docs, Google Calendar, Google Voice, Google Drive, Google Blogger, and Google Hangouts and any other online storage accessible by a user associated with the SUBJECT ACCOUNT.

g. All date, time and IP Addresses for each uploaded and download file as well as all Share settings for Google Picasa, Google Docs, Google Drive, Google Blogger and any other online storage accessible through the SUBJECT ACCOUNT.

h. For the SUBJECT ACCOUNT, provide the MAC address, and any additional identifiable information, for any and all devices utilized to access the SUBJECT ACCOUNT, and or any SUBJECT ACCOUNT Google services, to include but not limited to; IMEI/MEID, make and model, serial number, date and IP of last access to Google, IP Session logs, and a list of all accounts and or services that have ever been active on the device or devices.

i. All previously preserved data in the account to include what is detailed in paragraphs a-g above.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 2252A that have been committed, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Communications, images or videos related to the solicitation or production of images depicting minors engaging in sexually explicit conduct; or

b. Evidence of the possession, receipt, production or distribution of images depicting minors engaging in sexually explicit conduct; or

c. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

STATE OF NEW YORK)
COUNTY OF MONROE) SS:
CITY OF ROCHESTER)

JUSTIN BURNHAM, being duly sworn, deposes and says:

1. I am a Special Agent ("SA") with the Department of Homeland Security ("DHS"), United States Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"), and am presently assigned to the HSI Buffalo, NY office. I have been employed as a federal law enforcement officer since September 2001. I successfully completed the Federal Criminal Investigator Training Program as well as the US Customs Special Agent Training Program at the Federal Law Enforcement Training Center. Through my training, experience, and interaction with other Special Agents and law enforcement entities, I am familiar with the methods of operation used by people who are involved with offenses involving the sexual exploitation of children, to include the use of the Internet to further those offenses. I have assisted, participated, and supported numerous investigations involving offenses related to the sexual exploitation of children, including conducting arrests, preparing and executing search warrants, and conducting surveillance. I am familiar with the facts and circumstances of this investigation because of my participation and discussions with other law enforcement officers involved with this investigation.

2. This affidavit is submitted in support of a warrant to search the Google account of "daviddblasczak" and its associated email address of "daviddblasczak@gmail.com," hereinafter the SUBJECT ACCOUNT; one iPhone 4,

Model# A1349, FCC ID: BCGE2422B, which is black and silver in color; and one iPhone 5S, FCC ID: BCGE2642A, Model# A1533, IMEI# 536965064366192, which is black in color, (hereafter the "SUBJECT PHONES"), all of which are more fully described in Attachment A. The items to be seized include evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251(a) (production of child pornography), 2252A(a)(2) (receipt and distribution of child pornography), and 2252A(a)(5)(B) (possession of child pornography), as specified in Attachment B.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is submitted for the limited purpose of establishing probable cause for the requested search warrants and does not include each and every fact known to me concerning this investigation.

4. In March 2012, HSI Phoenix initiated an investigation into a password-protected, fee-based "Website M"[1] after a consensual interview with a suspect in a child exploitation investigation ("S1"). The interview resulted in HSI agents assuming S1's online identity on Website M, which is a closed site that can only be accessed by members

[1] The actual name of Website M is known to law enforcement. However, the investigation into the users of Website M remains ongoing, and the disclosure of the name of Website M would potentially alert their members to the fact that law enforcement officers are investigating Website M. Public disclosure of that fact is likely to provoke members to notify other members of the investigation, flee, and/or destroy evidence. Accordingly, to preserve the confidentiality and integrity of the ongoing investigation, the actual names and other identifying details of Website M are not disclosed in this affidavit.

who were provided login information by Website M.[2] HSI Phoenix SAs determined that Website M advertises files of child exploitative material for purchase.

5. Results from the preliminary investigation indicated that Website M was being hosted on a server physically located in India, and the website claimed to offer 600,000 images and 400 hours of video, all of which could be downloaded for a fee as compressed, encrypted files (.RAR files). Website M typically charged $89.99 USD for each .RAR file. Once downloaded, the user could "un-compress" the .RAR file to reveal multiple image and/or video files. It appeared to HSI Phoenix SA Nicole Rye that most of the .RAR files contain between 500 and 2,000 image and/or video files. Law enforcement agents who visited Website M estimated that many of the images and videos advertised on the website depict pre-pubescent male and female minors engaged in sexual activity with adults and/or posed in a sexually explicit manner.

6. According to SA Rye, Website M allows members to preview samples of the images/videos contained in the .RAR file prior to purchasing the .RAR file. Over the course of their investigation, which has involved previewing and downloading multiple .RAR files, law enforcement has found that the "sample" images/video screenshots SAs previewed always corresponded to the un-compressed image and video files contained in the downloaded .RAR file.

7. After selecting an encrypted .RAR file, the member pays for its password by entering in credit card information. Website M then causes an email to be sent to the

[2] S1 provided SAs with the URL link to Website M and S1's login information to Website M but S1 has not provided sufficient information to law enforcement to understand how S1 originally obtained the URL or login information for Website M.

member with the encryption password for the .RAR file. The member must enter that password to decrypt and un-compress the .RAR file.

8. I have been informed by SA Rye that, as a result of the interview with S1, law enforcement obtained membership information to Website M that allowed law enforcement to pose as S1 on the website. Between April 2014 and May 2017, SAs made multiple undercover purchases of .RAR files from Website M.

9. For example, in April 2014, SAs (posing as S1) successfully downloaded .RAR files from Website M. SAs reviewed the un-compressed image files and, based upon an analysis of hash values, law enforcement determined that the purchased files included video and image files from what law enforcement refer to as the "Jenny" series. The United States-based National Center for Missing and Exploited Children has identified and verified that the images from the "Jenny" series images depict a pre-pubescent minor child who appears to be less than ten years of age. Purchased files included the following video and image files of "Jenny":

a) "180-2.AVI 9Yo Jenny licked by dog. 16min./with sound." The screenshot for this video depicts a nude, blindfolded, pre-pubescent female who appears to be less than ten years of age lying on her back while a dog licks her genitals; and

b) Over twenty pictures from the "Jenny" series including an image of the same pre-pubescent, nude, female performing fellatio on a dog.

10. On May 26, 2017, an HSI Phoenix SA, working in an undercover capacity purchased a .RAR file from Website M titled "SIBERIAN MOUSE #36." The un-compressed files contained in the .RAR file depicted what appeared to be minors engaged in

sexually explicit acts. When the SA purchased the SIBERIAN MOUSE #36" file, the SA received a confirmation email from an email address from a U.S. payment processor, hereinafter PAYMENT PROCESSOR, stating that "Your order is currently being processed." The identity of the PAYMENT PROCESSOR is known, but is being left out of this affidavit due to the ongoing investigation of Website M and the PAYMENT PROCESSOR.

11. According to SA Rye, HSI Phoenix SAs initiated an investigation into the link between the PAYMENT PROCESSOR and Website M. The PAYMENT PROCESSOR was identified as a payment processor and online business management tool used by Website M.

12. On July 31, 2017, a Federal Magistrate for the District of Arizona signed a search warrant for the electronic documents in the possession of the PAYMENT PROCESSOR related to their business transactions with and on behalf of Website M.

13. On August 11, 2017, the PAYMENT PROCESSOR provided several spreadsheets in compliance with the search warrant. One of the spreadsheets listed all the transactions that had been processed by the PAYMENT PROCESSOR on behalf of Website M. This list included over 1,000 purchases made to Website M.

14. In September 2017, SA Rye analyzed the PAYMENT PROCESSOR records and identified individuals who made multiple purchases from Website M. The PAYMENT PROCESSOR records indicate that David Blasczak ("BLASCZAK") made approximately ten purchases from Website M between September 2015 and April 2017. According to the PAYMENT PROCESSOR records, the email address to which it sent the auto-generated

receipts and passwords for purchases made by BLASCZAK on Website M was blasczakd@gmail.com.[3]

15. In response to a summons, PayPal Holdings, Inc. provided the following subscriber information associated with the David Blasczak purchaser:

First Name: David
Last Name: Blasczak
Email: blasczakd@gmail.com
Address: 113 Jason Drive, Newark, NY, 14513
4 West Genesee Street, Clyde, NY, 14433
2 West Genesee Street, Clyde, NY, 14433
Frequent IP Addresses: 98.10.10.158 (SUSPECT IP ADDRESS).

16. In response to a summons, Charter Communications provided information that between February 17, 2017 through April 11, 2017, the SUSPECT IP ADDRESS was subscribed to David Blasczak 113 Jason Drive, Newark, NY.

17. Based upon the PAYMENT PROCESSOR records, law enforcement generated the following list of BLASCZAK's purchases made via the PAYMENT PROCESSOR from Website M along with identifying information linked to each purchase:

Date	Title	First Name	Last Name	Email	Phone	Region	Postal
9/23/2015	PHP SCRIPT 153	David	Blasczak	blasczakd@gmail.com	3154813450	NY	14513
2/17/2017	PHP SCRIPT 347	David	Blasczak	blasczakd@gmail.com	3154813450	NY	14513
2/19/2017	PHP SCRIPT 133	David	Blasczak	blasczakd@gmail.com	3154813450	NY	14513
2/19/2017	PHP SCRIPT 218	David	Blasczak	blasczakd@gmail.com	3154813450	NY	14513
2/21/2017	PERL SCRIPT 113	David	Blasczak	blasczakd@gmail.com	3154813450	NY	14513
2/22/2017	AJAX SCRIPT 79	David	Blasczak	blasczakd@gmail.com	3154813450	NY	14513
3/3/2017	AJAX SCRIPT 83	David	Blasczak	blasczakd@gmail.com	3154813450	NY	14513
4/8/2017	PHP SCRIPT 269	David	Blasczak	blasczakd@gmail.com	3154813450	NY	14513
4/10/2017	AJAX SCRIPT 27	David	Blasczak	blasczakd@gmail.com	3154813450	NY	14514

[3] "blasczakd@gmail.com" was the subject of a search warrant issued by US Magistrate Jonathan Feldman on January 16, 2018. The SUBJECT ACCOUNT in this application is ("daviddblasczak@gmail.com"), a different Google account as further described below.

4/11/2017	PHP SCRIPT 412	David	Blasczak	blasczakd@gmail.com	3154813450	NY	14513

18. After obtaining BLASCZAK's purchase history from the PAYMENT PROCESSOR, an HSI Phoenix SA, in an undercover capacity, viewed "samples" from each file titled in BLASCZAK's purchase records from Website M. The previews were recorded using screen capture software available to law enforcement. I have reviewed previews from some of the files referenced in the table above, which BLASCZAK downloaded. Based on my review they contain child pornography as defined by Title 18, United States Code, Section 2256(8).

19. Specifically, on April 11, 2017, BLASCZAK purchased a .RAR file with the billing code "PHP SCRIPT 412." SAs located a .RAR file on Website M titled "HM VIDEO ARCHIVE 412." When SAs clicked on this .RAR file on Website M, the website provided the following prompt at the bottom of the webpage "BUY NOW PASSWORD FOR HM VIDEO ARCHIVE" #412." When SAs clicked on this prompt, the webpage displayed an option to buy "PHP SCRIPT 412" with an "Immediate License Code sent by Email. I reviewed the screen capture of the "samples" viewed from PHP SCRIPT 412 file. Two of the image files are described below:[4]

a) The first image depicts a pre-pubescent, Caucasian minor female who appears to be less than ten years of age sitting on a couch and wearing what appears to be a bathrobe. The child's right hand is touching her genitals and the focus of the picture is on her genitals and chest.

[4] The image files are not associated with individual file names because they were previewed as "samples." If law enforcement had downloaded the .RAR file, the un-compressed files would contain individual file names. Law enforcement elected not to download all of the .RAR files purchased by BLASCZAK because law enforcement was concerned that such a large volume of purchases would be suspicious to Website M and may cause Website M to terminate S1's membership.

b) The second image depicts a pre-pubescent female Caucasian child who appears to be less than 8 years of age. There is an adult male penis inserted into her mouth.

20. In addition, on April 10, 2017 BLASCZAK purchased a .RAR file with the billing code "AJAX SCRIPT 27." SAs located a .RAR file on Website M titled "NU PHOTO ARCHIVE 27, Pre-Teen Hardcore #8. 2020 images." When SAs clicked on this .RAR file on Website M the webpage displayed an option to buy "AJAX SCRIPT 27" with an "Immediate License Code sent by Email." I reviewed the screen capture of the "samples" viewed from AJAX SCRIPT 27 file. Two of the image files below:

a) The first image depicts a pre-pubescent, Caucasian minor[5] who appears to be less than ten years of age sitting thigh to thigh with an adult male. The genital area of the child is touching the adult male. The minor child is holding the adult male's penis in the child's hand.

b) The second image depicts a Caucasian female who appears to be less than ten years of age sitting on her knees on top of a blanket. The lower body of an adult male is visible and he appears to be standing over the female child. The adult male's penis is inserted into the child's mouth.

21. I reviewed the financial purchase records provided by the PAYEMNT PROCESSOR and noted that BLASCZAK's purchases listed his billing address as 113 Jason Drive, Newark, NY.

22. Based on the above, a search warrant was signed on January 16, 2018 by Hon. Jonathan Feldman, United States Magistrate Judge, authorizing a search of 113 Jason Dr., the home of BLASCZAK.

[5] Due to the close up nature of the photo it is not possible to tell if the minor is male or female.

23. On January 18, 2018, Agents from HSI, accompanied by members of the New York State Police, executed the above-described search warrant at 113 Jason Drive. Upon executing the warrant, Agents located several digital devices including a laptop, a digital camera, multiple SD cards, multiple thumb drives, and 2 sandisk memory sticks. One of the devices is an "Infinitive" 64 gigabyte USB thumb drive, serial number BN160625517B, found in a brief case near the front entranceway of the residence. An HSI Computer Forensic Agent (CFA), previewed the contents of the thumb drive on scene and immediately discovered images and videos of child pornography involving prepubescent minors. At the time of this writing, the CFA already discovered approximately 10 gigabytes of files on the subject thumb drive containing suspected child pornography. I have described two of the images and one video below:

a) Image file located in "folder 01," jpg. file "2," created 9/6/17, which depicts a prepubescent female with her legs spread, inserting her fingers into her vagina;

b) Image file located in "folder 01," jpg. file "2011-05-24_12-42-53_Zdjcie0061," created 9/6/17, which depicts a prepubescent female, approximately 2 years of age performing oral sex on an adult male. The male's penis is seen in the child's mouth;

c) Video file located in "folder 362 vid," .avi file "362-7," created 2/12/17, which depicts an adult male performing oral sex on a prepubescent female. The female appears to be approximately 3 years of age and the males mouth can be seen in contact with the child's vagina.

24. Agents estimate that they have already discovered in excess of 1,000 images and multiple videos of child pornography on the subject thumb drive. The thumb drive and other digital devices are currently being transported to HSI Buffalo for a full forensic review.

25. BLASCZAK was present during the execution of the search warrant and was interviewed by HSI SAs Justin Burnham and Nicole Rye. The interview took place in SA Burnham's vehicle outside of the residence. During that interview, BLASCZAK initially

denied having any images or videos of child pornography. He then admitted to being the sole owner and user of the email account and credit card associated with receipt of child pornography through Website M (blasczakd@gmail.com). As the conversation progressed, BLASCZAK acknowledged that he owned a thumb drive that contained images and videos of child pornography. He then directed Agents to the brief case and thumb drive described above. BLASCZAK admitted that he purchased child pornography over the internet, and that the website that he purchased child pornography from required that he create an account containing a username and password. BLASCZAK admitted that he would pay approximately $100 per file that he purchased. It should be noted that since Website M sold compressed files, it is estimated that each "file" BLASCZAK purchased for $100 would have contained thousands of images and/or videos. BLASCZAK estimated that the children depicted in the child pornography that he purchased were between 5 and 10 years of age. BLASCZAK specifically used the word "prepubescent," when asked the ages of the children depicted in the videos and images he possessed. BLASCZAK told Agents that he possessed more than 50 videos and hundreds of images on the aforementioned thumb drive. When asked what his favorite type of child pornography was, BLASCZAK stated "oral."

26. As the conversation continued, BLASCZAK acknowledged that he works as a physician and treats children at his office located at 4 West Genesee Street, Clyde, NY, 14433. BLASCZAK denied ever abusing any of his child patients, but admitted to Agents that he previously photographed the genitals of children at his office. When asked, BLASCZAK claimed that he was conducting his own independent research about child sex abuse and paid the parents of approximately 8 children to photograph the children's genitals. BLASCZAK told Agents that he told the parents that he was conducting medical

research. BLASCZAK admitted that he was not sanctioned by a hospital, university, medical organization or any other professional medical board to photograph children's genitals. He claimed that he took the images for "teaching purposes" but admitted that he kept the photographs for himself for his "own gratification." BLASCZAK said that the photographs were taken years ago, but that he maintained some photographs of children's genitals in a "teaching" file in his office at his office at 4 West Genesee Street, Clyde, NY, 14433. BLASCZAK provided a written consent to the seizure of these items.

27. BLASCZAK thereafter accompanied agents to NYSP Lyons, where he continued to be interviewed. There, BLASCZAK made further admissions, including to engaging in sexually abusive behavior against his (deceased) daughter's minor friends during sleepovers. BLASCZAK stated that he touched his daughter's minor friends while they were sleeping and photographed them. BLASCZAK admitted to being sexually aroused by his daughter's friends. BLASCZAK also admitted that he has masturbated to the photographs that he took of his child-patients at his medical practice.

28. Based on the above, a Criminal Complaint was signed by Hon. Jonathan Feldman, United States Magistrate Judge, charging BLASCZAK with Receipt and Possession of Child Pornography in violation of Title 18, United States Code, Sections 2252A(a)(2)(A) and 2252A(a)(5)(b). BLASCZAK was arrested on January 18, 2018.

29. Following BLASCZAK's arrest, HSI was contacted by witness, W1, who resided with BLASCZAK at 113 Jason Drive. W1 became aware of the nature of BLASCZAK's charges, and desired to assist law enforcement in determining whether BLASCZAK may have produced, possessed or received child pornography at 113 Jason

Drive or on any of his devices about which W1 had knowledge. During the conversation, W1 reported to Agents that BLASCZAK owns the following phones: One iPhone 4, Model# A1349, FCC ID: BCGE2422B, which is black and silver in color; and one iPhone 5S, FCC ID: BCGE2642A, Model# A1533, IMEI# 536965064366192, which is black in color (hereafter the "SUBJECT PHONES").

30. W1 reported that the iPhone 4 was utilized by BLASCZAK up until he sold his practice identified as Arcadia Family Practice. Upon beginning his new practice at Clyde Family Health Clinic, BLASCZAK'S phone was upgraded to the iPhone 5S. W1 advised that he assisted BLASCZAK in setting up the iPhone 5S, one of the SUBJECT PHONES. W1 advised that when he set up the BLASCZAK'S phone, he activated an auto archive back-up of the device such that any and all images and videos would be backed up to the cloud. He stated that if a picture was taken and deleted seconds later, the picture would still be backed up to the cloud. The Google account used to set up the backup was "daviddblasczak" with associated email address "daviddblasczak@gmail.com," the SUBJECT ACCOUNT. As noted above, this is a different Google account than was the subject of the January 16, 2018 search warrant signed by the Hon. Jonathan Feldman. W1 reported that the cloud service utilized to back up the SUBJECT PHONES, was Google Drive, which would be linked to the SUBJECT ACCOUNT.

31. Based on the above, W1 is concerned that BLASCZAK likely used the SUBJECT PHONES to engage in the possible production, receipt, and distribution of child pornography. W1 stated that evidence of any pictures taken by BLASCZAK would still be present on the SUBJECT ACCOUNT, which acted as the backup to the SUBJECT PHONES, even if deleted. W1 requested to turn the SUBJECT PHONES over to HSI for

analysis. Based on your Affiant's training and experience, W1 is correct that if the SUBJECT PHONES were backed up by the SUBJECT ACCOUNT, photographs taken by the SUBJECT PHONES, may still be available to law enforcement. In addition, current forensic tools may allow HSI CFA's to recover images from the SUBJECT PHONES even if they were deleted.

32. On January 23, 2018, HSI Agents met W1 in Newark, NY at which point W1 provided Agents with the SUBJECT PHONES.

33. In addition to the above, on January 19, 2018, HSI was contacted by the Newark Police Department, who reported having investigated BLASCZAK in September 2015 for photographing the vaginal area of a kindergarten student during a school orientation. Specifically, on September 2, 2015, the Newark Police Department investigated BLASCZAK when it was reported by a parent that BLASCZAK was observed taking pictures up a kindergarten student's dress while she was sitting across from BLASCZAK. BLASCZAK was interviewed, but denied engaging in any misconduct. Police did not locate any photographs depicting the female student based on a cursory review of digital items on BLASCZAK'S person. The police, however, did observe that BLASCZAK was in possession of an iPhone matching the description of the SUBJECT PHONES. This phone was not seized and was never subjected to a forensic analysis. BLASCZAK was not investigated further for this incident. Based on the above, there is probable cause to believe that evidence of photos taken by BLASCZAK may be present on the SUBJECT PHONES or in the SUBJECT ACCOUNT.

34. Based on my training and experience, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who view and possess multiple images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a) Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or in other visual media; or from literature describing such activity.

b) Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, including online accounts, such as the SUBJECT ACCOUNT, and devices such as the SUBJECT PHONES. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c) Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer or on an online account, such as the SUBJECT ACCOUNT or the SUBJECT PHONES. These collections are kept to enable the individual to view the collection, which is valued highly.

d) Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

e) Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

f) Individuals can use online resources to retrieve, store and share child pornography, including services offered by Internet Portals such as Google, America Online (AOL), Yahoo! and Hotmail, among others, including the SUBJECT

ACCOUNT. Online services allow a user to set up an account providing e-mail and instant messaging services, as well as electronic storage of cellular telephone files in any variety of formats. A user can set up an online storage account from any cellular telephone with access to the Internet. Evidence of such online storage of child pornography is often found within the online storage account.

35. Based on my training and experience, including conversations with other law enforcement officers, I have learned the following about Google, Inc. and other electronic internet service providers:

a) Google provides a variety of on-line services, including electronic mail ("electronic mail") access, to the general public. Google allows subscribers to obtain electronic mail accounts at the domain name "gmail.com", like the email account listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and un-retrieved electronic mail for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, electronic mail transaction information, and account application information.

b) In general, an electronic mail message that is sent to a Google subscriber is stored in the subscriber's "in-box" on Google servers until the subscriber deletes the electronic mail. If the subscriber does not delete the message, the message can remain on Google servers indefinitely. The user can move and store messages in personal folders such as a "sent folder." In recent years, Google and other internet service providers have provided their users with larger storage capabilities associated with the user's email account. Google and other internet service providers have allowed users to store up to 30 gigabytes of information associated with the account on the respective internet service provider's servers. Based on conversations with other law enforcement officers with experience in executing and reviewing search warrants of electronic mail accounts, I have learned that search warrants for electronic mail accounts and computer systems have revealed stored emails sent and/or received many years prior to the date of the search.

c) When the subscriber sends an electronic mail, it is initiated at the user's computer or other electronic device such as a cellular telephone, transferred via the Internet to Google's servers, and then transmitted to its end destination. Google often saves a copy of the electronic mail sent to the users account automatically. Unless the sender of the electronic mail specifically deletes the electronic mail from the Google server, the electronic mail can remain on the system indefinitely.

d) A sent or received electronic mail typically includes the content of the message, source and destination information, the date and time at which the electronic mail message was sent, and the size and length of the electronic mail message. If an electronic mail user writes a draft message but does not send it, that message may also be saved by Google but may not include all of these categories of data.

e) A Google subscriber can also store files, including electronic mails, address books, contact or buddy lists, calendar data, pictures, and other files on servers maintained and/or owned by Google. Subscribers to Google might not store, on their home computers, copies of the electronic mails stored in the Google account. This is particularly true when they access their Google account through the web, or if they do not wish to maintain particular electronic mails or files in their residence.

f) In general, internet service providers offering electronic mail services like Google ask each of their subscribers to provide certain personal identifying information when registering for an electronic mail account. This information may include the subscriber's full name, physical address, telephone numbers and other identifiers, such as alternative electronic mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). It should be noted that often times internet service providers do not verify the information provided to ensure that the individual providing the information is being truthful, nor do they require the individual to provide all of the information mentioned above.

g) Electronic mail providers typically retain certain transaction information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website), and other log files that reflect usage of the account. In addition, electronic mail providers often have records of the Internet Protocol (IP) address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other electronic devices were used to access the electronic mail account.

h) In some cases, electronic mail account users will communicate directly with an electronic mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Electronic mail providers typically retain records about such communications, including records of contacts between the user and the providers support services, as well as records of any actions taken by the provider or user as a result of the communications.

i) In my training and experience, evidence of who was using an electronic mail account may be found in address books, contact or "buddy" lists, electronic mail

messages in the account, and attachments to electronic mails messages, including pictures and files.

j) Google users have access to various Google services that can be used to store various types of data such as Gmail , Google Picasa, Google+, Google Earth, Google Docs, Google Calendar, Google Voice, Google Drive, Google Blogger, and Google Hangouts.

36. Based on the foregoing, I believe there is probable cause to believe that evidence, fruits, and instrumentalities of the violations of 18 U.S.C. §§ 2251(a) (production of child pornography), 2252A(a)(2) (receipt of child pornography), and 2252A(a)(5)(B) (possession of child pornography), as described above and in Attachment B of this affidavit, will be found in a search of the SUBJECT ACCOUNT and SUBJECT PHONES as further described above and in Attachment A of this affidavit.

JUSTIN BURNHAM
Special Agent
Homeland Security Investigations

Subscribed to and sworn before me
this 26 day of January, 2018.

JONATHAN W. FELDMAN
United States Magistrate Judge